netSecurity Forensic Labs

| e-Discovery | Forensics | Incident Response |

NetSecurity® Corporation
Inno Eroraha, Chief Strategist
22375 Broderick Drive
Suite 235
Dulles, VA 20166

SBA 8(a) Certified SDB

GSA Contract # GS-35F-0288Y

VA DCJS # 11-5605

Phone: 703.444.9009 / 1.855.NETSECURITY
Toll Free: 1.866.664.6986
Web: www.netsecurity.com
Email: forensics@netsecurity.com


cingular
9:41 AM
Text
Calendar
Photos
Camera
Calculator
Stocks
Maps
Weather
Notes
Clock
Settings
Phone
Mail
Web
iPod


BlackBerry


10:05 am 1/24

The Landscape

Digital information continues to grow at an exponential rate. Data is no longer stored solely in computer hard drives, backup tapes, or compact discs (CDs). With the growth of emerging portable data and storage devices, such as portable digital assistants (PDAs), cell phones, and Blackberry devices, crucial information can be anywhere and easily passed from device-to-device. Information stored in these changing media can be crucial sources of evidence in corporate, civil, and criminal investigations.

Digital forensics is the process of acquiring, preserving, analyzing, and producing digital evidence. Forensics is required to determine if evidence exists, such as in incidents involving: intellectual property theft, network hacking, evidence tampering, employee misuse of computer, illicit pornography, policy violation, electronic harassment, and other digital crimes.

Forensic investigation is a time-consuming effort that requires specialized expertise, procedures, tools, and lab environment. Proper investigation and evidence collection focused on forensically sound processes, is an absolute necessity. This ensures that the forensic process can withstand the scrutiny of an opposing legal counsel. Rest Assured. NetSecurity® Corporation helps you reach your digital forensics goals, promptly and cost-effectively.

Corporate Overview

NetSecurity® Corporation is a digital forensics, cyber security consulting and training company. We work with you to understand the unique goals and requirements of your business.

- Our **hands-on security solutions** protect you against emerging security threats and help you manage your enterprise security risk proactively
- **NetSecurity Forensic Labs** delivers solutions that help you acquire, preserve, analyze, and produce digital evidence promptly
- Our proprietary **Hands-On How-To®** training program provides you with the knowledge of real-world security issues through simulation and "how-to" exercises that enable you to do your job successfully

Selected Clients

Public and private sector organizations continue to rely on NetSecurity to help them overcome their security and investigation challenges. A select list of customers includes:

Public Sector Clients

- Internal Revenue Service
- Department of Homeland Security
- Department of Defense
- United States Navy
- United States Marine Corps
- Veterans Affairs
- Department of Commerce
- National Institutes of Health

Private Sector Clients

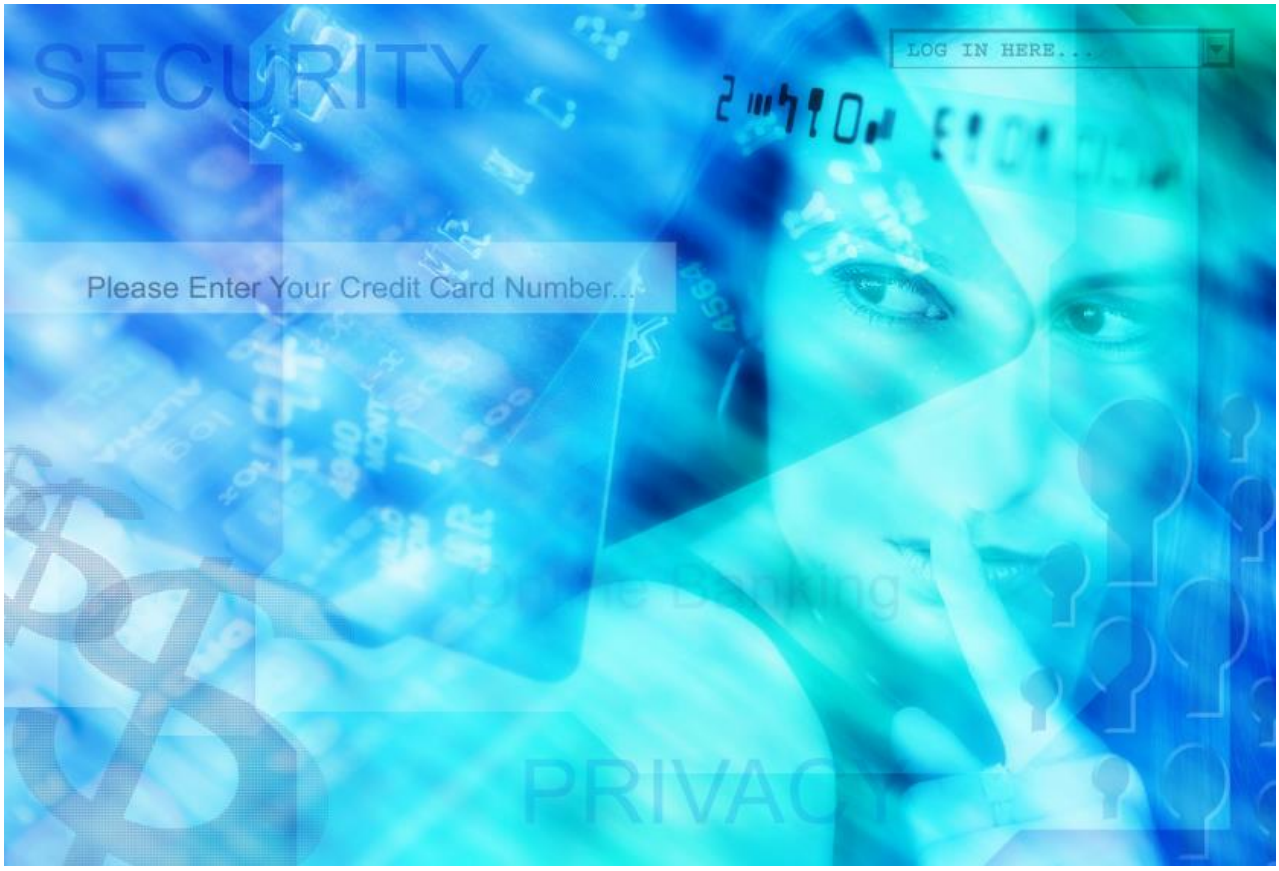
- Major Hospital System
- One of the Largest Hospitality Chains
- Publicly-traded Financial Institutions
- Academic and Training Institutions
- Prestigious Law Firms
- Major Federal Integrators/Contractors
- Private Investigation Firms

NetSecurity's Benefits

NetSecurity brings unparalleled expertise to guide you through the investigation of computer crimes and in delivering impeccable results in security engagements. Our experts have worked in various establishments, including: The Pentagon, Navy, Marine Corps, IRS, DHS, VA, other Federal agencies, and publicly-traded companies. Our clients continue to rely on us because:

- We have a breadth of experience in computer security, privacy, and audit of a variety of information technology environments.
- Our forensic experts have worked in highly classified projects within DoD and other U.S. Federal agencies.
- We ensure and preserve the confidentiality of your case, investigation, and engagement.
- Our rapid response capability ensures you get the right information, timely, efficiently, and cost-effectively.
- We deliver unmatched customer service and quality results.
- NetSecurity Forensic Labs is equipped with state-of-the-art tools and technologies to excavate data from the latest storage devices and produce admissible results.
- We teach the latest forensics tools and techniques of the trade, using real-world scenarios.
- Our professionals have years of experience and have certifications in: CISSP, ISSAP, ISSMP, CISM, CISA, CHFI, etc.
- We avoid conflict of interest and are vendor neutral in the choice of our tools.

NetSecurity's Expertise

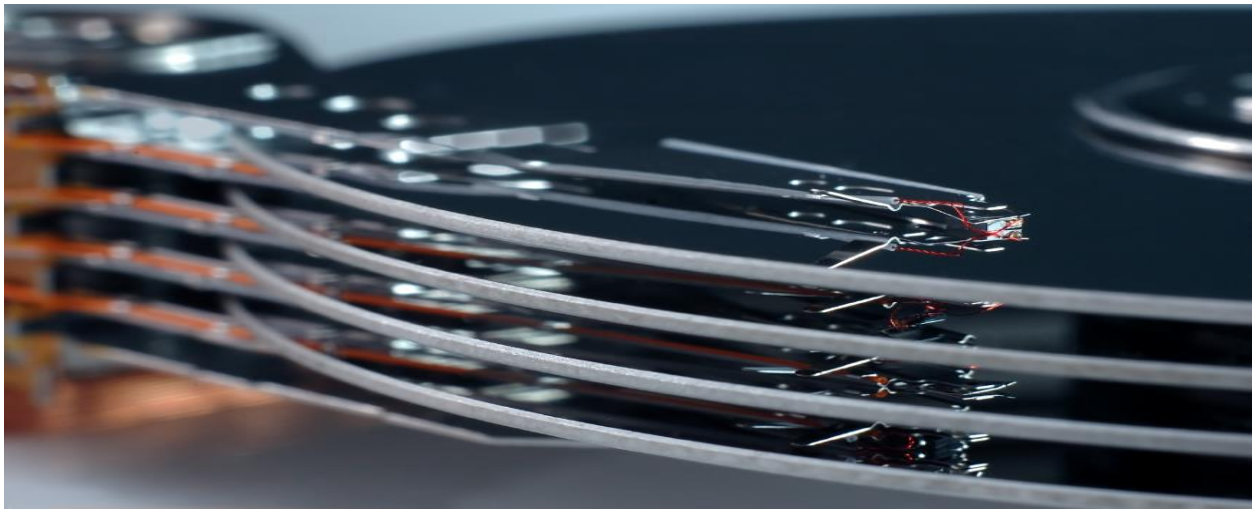


Digital forensics expertise requires more than an in-depth familiarity with the latest tools and technologies of the trade. Forensics requires deep experience with computer architecture, operations, operating systems internals, network operations, and storage systems and components. Further, experience in computer security and hackers' techniques provide a solid foundation.

NetSecurity's engineers, researchers, analysts, and forensic experts have proven skills in auditing, privacy, risk management, security assessment, penetration testing, computer security, systems administration, database systems, email administration, wireless networks, and complex network design and operation. We leverage our deep knowledge in these areas ensuring that "no stone is left unturned" during each forensic investigation. Our forensics and discovery methods make certain that collected evidence can stand the rigors of legal scrutiny.

- Ethical hacking
- Intrusion Detection Systems (IDS)
- Centralized log infrastructure
- Routers, firewalls, Unix, Windows, Macintosh, etc.
- Portable storage devices
- Live forensic data collection
- Internal Audit
- Information Privacy
- Risk Assessment
- Computer Security
- System/Network Administration and Operation
- Wireless networks

NetSecurity's Forensic Solutions



NetSecurity Forensic Labs is a state-of-the-art, secure forensics facility equipped with leading-edge tools and technologies of the trade. NetSecurity Forensic Labs provides cost-effective solutions in electronic discovery (e-discovery), incident response, digital forensics, and training.

e-Discovery

Through NetSecurity's e-discovery solutions, we help you search, locate, and secure electronic information for use as evidence in civil or criminal litigation. We work with you to identify, collect, preserve, recover, and produce electronic data to ensure that you comply with e-discovery requests promptly. Our vendor-neutrality ensures that the most cost-effective e-discovery strategy is executed.

We gather electronic data from storage devices that serve as evidence from all file types, including: text, emails, chat, images, calendar files, databases, spreadsheets, audio files, servers, and computer applications.

Cyber Incident Response

Many companies have crisis management plans to cover natural disasters or unexpected employee concerns. However, it is also important to be prepared to handle information security incidents before any occur. A well-executed response can reveal the true extent of a compromise and prevent future occurrences.

Our analysts have created methodologies to evaluate, mitigate, escalate, and contain incidents. We assist you in the creation, implementation, and rollout of your incident response capability. NetSecurity also helps you create policies and processes to ensure that security incidents are resolved effectively in the least amount of time.

In addition, NetSecurity has well equipped and experienced incident responders with years of experience in information security intrusion detection. We help investigate systems, networks, operating systems, database systems, and other infrastructure components. NetSecurity is extremely nimble, which ensures that we respond to any security incident quickly. We take the additional step of securing the compromised system, forensically preserving the data, and analyzing the evidence to determine the perpetrator.

Digital Forensics Investigations

NetSecurity Forensic Labs works with you to investigate computer systems and determine whether they have been used for criminal or unauthorized civil activities. We conduct forensic recovery and analysis on desktops, servers, systems, network devices, and removable media in a wide variety of formats.

- Evidence/data acquisition, preservation, recovery, analysis, and reporting
- Intellectual property theft
- Computer misuse
- Corporate policy violation
- Mobile device (PDA, cell phone) data acquisition and analysis
- Malicious software/application
- System intrusion and compromise
- Encrypted, deleted, and hidden files recovery
- Illicit pornography
- Confidential information leakage

Using our techniques, we recover deleted/hidden/encrypted files, construct system usage activity, and determine whether an intruder has compromised a computer. Further, we help determine the data that the attacker modified, accessed, copied, or deleted. Our forensics investigations are focused on obtaining and reconstructing activities from data in various storage media:

- Computer networks
- Email systems
- Database management systems
- Handheld devices (PDA, iPad, iPod, Blackberry, smart phones, etc.)
- Backup tapes, and other internal/external storage media

Hands-On How To® Forensic Training

NetSecurity provides **Hands-On How-To®** training in digital forensics. Our real-world simulated scenarios demonstrate "how-to" conduct forensic investigations. Our current training courses include:

- Hands-On How-To® Computer Forensics
- Hands-On How-To® Computer Forensics for Attorneys (CLE Credit)
- Hands-On How-To® Incident Response
- Hands-On How-To® Malware Analysis
- Hands-On How-To® Memory Forensics
- Hands-On How-To® Malicious Document Analysis

NetSecurity's Approach

Proper forensics investigation and data collection focused on sound processes and techniques ensure that evidence produced is admissible in a court action or corporate investigation. NetSecurity's forensic experts follow techniques that withstand the scrutiny of litigation.

Our professionals have deep experience in ethical hacking, securing complex systems and networks, auditing information systems, and responding to security incidents. We have experience in investigating real network attacks and employee misuse of information resources. NetSecurity helps you answer the questions of who, what, when, where, why, and how about computer-related incidents. Further, we peer-review our work and reports to ensure clarity and ease of understanding by a non-technical audience. Also, we use more than one forensic tool to verify our work, ensuring that we produce accurate results.

Forensic investigation is a time-consuming task requiring attention to details, specialized expertise, procedures, tools, and environments. NetSecurity Forensic Labs is equipped with appropriate tools and technologies that can find evidence in both current and older computer storage technologies. We follow proper forensics investigation and evidence collection processes, such as: physical isolation of the target system to ensure data integrity, preventing evidence contamination, and performing a bit-by-bit duplication of the original source storage media. We also follow strict technical procedures to ensure that evidence is admissible in regulatory compliance, litigation, and corporate investigations.

At NetSecurity, we assume the worst-case scenario and treat each forensic project as if it will end up in court and undergo legal scrutiny. We maintain a strict chain of custody and stringent evidence control procedures. We combine our hands-on approach to information security with our in-depth experience in electronic discovery, incident response, and digital forensics to help you overcome cost-prohibitive forensic engagements.

Corporate Identification

- **Corporate Status:** Incorporated
- **Year Founded:** 2004
- **Certification/Classification:**
  - 8(a) Business Development
  - Small Disadvantaged Business
- **Tax ID (EIN):** 54-1945426
- **DUNS:** 122657005
- **NAICS Codes:** 541199, 541511, **541512**, 541513, 541519, **541690**, **611420**
- **CAGE Code:** 3CJJ4
- **SIC Code:** 7371, 7372, 7373
- **CCR Registration:** YES
- **Facility Clearance:** Contact us for details
- **Credit Card Acceptance:** Yes

Contract Vehicles

- 8(a) Sole Source Justification
- GSA Schedule (# GS-35F-0288Y)
- Navy Seaport-e (# N00178-07-D-5205)
- VETS GWAC (# GS-06F-0533Z)
- TIPSS-4 Small Business (SB) IDIQ
- TRICARE TEAMS IDIQ – *Pending*

Corporate Contact

NetSecurity® Corporation
Inno Eroraha, Chief Strategist
22375 Broderick Drive, Suite 235
Dulles, VA 20166
Email: forensics@netsecurity.com
Web: www.netsecurity.com
Phone: 703.444.9009
Fax: 703.444.6899
Toll Free: 1.855.NETSECURITY

netSecurity
Forensic Labs

netSecurity®